IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

MONEY AND DATA PROTECTION LIZENZ GMBH & CO. KG,	)	
Plaintiff,	)	C.A. No. 18-1477-CFC
v.	)	
DUO SECURITY, INC.,	)	
Defendant.	)	

PLAINTIFF'S ANSWERING BRIEF IN OPPOSITION TO DUO SECURITY, INC.'S MOTION FOR JUDGMENT ON THE PLEADINGS OF PATENT INVALIDITY UNDER 35 U.S.C. § 101

OF COUNSEL:

Scott T. Weingaertner
Stefan Mentzer
Leon Miniovich
WHITE & CASE LLP
1221 Avenue of the Americas
New York, New York 10020
Tel: (212) 819-8200

David E. Moore (#3983)
Bindu A. Palapura (#5370)
Stephanie E. O'Byrne (#4446)
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19801
Tel: (302) 984-6000
dmoore@potteranderson.com
bpalapura@potteranderson.com
sobyrne@potteranderson.com

Attorneys for Plaintiff Money and Data Protection Lizenz GmbH & Co. KG

November 5, 2019
6466369 / 45431

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND RULES

I. NATURE AND STAGE OF PROCEEDINGS

Money and Data Protection Lizenz GmbH & Co. KG ("MDPL") filed a complaint against Duo Security, Inc. ("Duo") alleging infringement of U.S. Patent No. 9,246,903 (the "'903 patent"). *See* D.I. 1. Duo filed a motion to dismiss under Rule 12(b)(6); Duo did not raise 35 U.S.C. § 101 as a basis for its motion. *See* D.I. 9. The Court denied the motion, and MDPL filed an amended complaint on September 30, 2019. *See* D.I. 15. Duo answered the complaint and moved for judgment on the pleadings on grounds of patent invalidity under § 101. *See* D.I. 16, 17. This is MDPL's answering brief in opposition to Duo's motion.

II. SUMMARY OF ARGUMENT

The claims of the '903 patent are patent-eligible under the *Alice* framework. MDPL does not claim to have invented authentication before the ancient Greeks, nor is it MDPL's position that that all developments in the field of authentication are eligible for patent protection. Rather, the '903 patent claims a specific improvement upon computer-implemented multifactor authentication technology increasing the efficiency of the system and relieving most of the burden on the user without compromising security. That solution is described in the specification of the '903 patent which, by law, is presumed valid. The claimed methods improve computer system functionality and are not directed to an abstract idea (*Alice* step 1). And the claims of the '903 patent improve upon the existing technology through a non-conventional arrangement of computer and mobile networking elements that amounts to significantly more than an abstract idea (*Alice* step 2).

Duo fails to establish, by clear and convincing evidence, the facts necessary to prove that the '903 patent is no longer valid. Rather, it sets up a straw man, arguing that the claims of the patent are directed to the broad, abstract idea of "authentication." In doing so, Duo oversimplifies what is claimed and ignores the actual language of the claims and their specific requirements. Duo also asserts facts outside of the pleadings to argue that the claims are directed to age-old concepts.

In doing so, Duo takes a position that is inconsistent with its prior representations to the USPTO that its own authentication-related patents claim patent-eligible subject matter. Duo may wish to take the opposite position now, but it cannot credibly argue that there are no issues of fact requiring the Court to find the '903 patent invalid on the pleadings. The '903 patent is not directed to an abstract idea, and it contains an inventive concept. The patent is valid.

III. STATEMENT OF FACTS

In today's world, the concept of authentication is integrated into computer technology, and the '903 patent claims a specific improvement to a particular authentication technique rooted in computer technology. *See* '903 patent at 1:54-56, 1:64-2:4, 2:30-32, 2:43-46. Multifactor authentication systems provide multiple layers of protection by requiring a user to provide two separate inputs to verify his or her identity. In a common example of a two-factor authentication system, the user attempts to log into email from a computer by providing a username and password (the first authentication factor), and is asked to input a code that has been sent via text message to a mobile phone (the second authentication factor). Typically, the more authentication factors required, the more secure the system. While additional authentication factors increase security of the system, requiring users to provide multiple inputs before verifying their identities can be burdensome, time-consuming, and costly to implement. A user may forget his or her password or input the incorrect code, transmission of messages to and from mobile devices may incur additional charges, and fingerprint or facial scanners may be expensive and not easily portable.

The '903 patent recognizes the disadvantages of conventional multifactor authentication systems and provides an elegant solution that improves authentication technology by relieving most of the burden on the user to remember a password or input the correct code. *See id.* at 1:54-2:32. Rather than requiring the user to retrieve information and input multiple authentication

factors, the user's identity is verified by (1) transmitting the user identification, such as a username, via a first communication channel, and (2) checking via a second communication channel that an authentication function is activated in the user's mobile device. By replacing manual entry of information for an authentication factor with a check for an activated authentication function, the '903 patent provides a more efficient system. For example, to activate the authentication function, the user may simply activate their mobile device (*id.* at 2:54-60), activate an app on a smartphone (*id.* at 6:59-62), or flip a switch on a key fob (*id.* at 8:42-49).

The '903 patent improves authentication technology by increasing the efficiency of computer-rooted technology without compromising the level of security of multifactor authentication systems, making it easier for the user to verify the user's identity. *See id.* at 1:54-2:32, 3:44-50. The claimed invention verifies a user's identity with fewer resources, less user interaction, and is compatible with simpler devices. *See id.* at 1:54-56.

IV. LEGAL STANDARD

While the ultimate determination of eligibility under § 101 is a question of law, "there can be subsidiary fact questions which must be resolved en route to the ultimate legal determination." *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1128 (Fed. Cir. 2018). "Any fact . . . that is pertinent to the invalidity conclusion must be proven by clear and convincing evidence." *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018). In considering a Rule 12(c) motion, a court must accept as true (1) all well-pleaded allegations in the non-movant's complaint and draw all reasonable inferences in the non-movant's favor (*see Zimmerman v. Corbett*, 873 F.3d 414, 417-18 (3d Cir. 2017)), and (2) all statements in the patent specification about the purported invention (*see MAZ Encryption Tech. LLC v. Blackberry Corp.*, C.A. No. 13-304-LPS, 2016 U.S. Dist. LEXIS 134000, at *15 (D. Del. Sept. 29, 2016)). Factual allegations taken as true can preclude the resolution of the eligibility question as a matter of law, considering

well-pleaded allegations in the non-movant's pleadings and drawing all reasonable inferences in the non-movant's favor. *See Aatrix Software*, 882 F.3d at 1125 (numerous and specific factual allegations suggested the claimed invention was directed to an improvement in the computer technology); *Berkheimer*, 881 F.3d at 1365 (Fed. Cir. 2018) (written description in conjunction with certain claims raised a factual dispute regarding the existence of an inventive concept). The Court may grant a Rule 12(c) motion only where "the movant clearly establishes that no material issue of fact remains to be resolved and [the movant] is entitled to judgment as a matter of law." *Rosenau v. Unifund Corp.*, 539 F.3d 218, 221 (3d Cir. 2008) (citation omitted).

Under 35 U.S.C. § 101, "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof" is eligible for patent protection. The Supreme Court has established a two-step framework for determining if a patent claims eligible subject matter under § 101. *See Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014). In the first step, a court considers whether the patent's claims are directed to a law of nature, natural phenomenon, or abstract idea. *See id.* at 2355. A court must articulate with "specificity" what the claims are directed to, *Thales Visionix, Inc. v. United States*, 850 F.3d 1343, 1347 (Fed. Cir. 2017), rather than "simply ask whether the claims *involve* a patent-ineligible concept," because "all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas," *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016) (citation omitted) (emphasis in the original). In particular, the claims should not be read "at such a high level of abstraction" that they become "untethered from the language of the claims," all but ensuring "that the exceptions to § 101 swallow the rule." *Id.* at 1337. The Federal Circuit specifically "cautioned that courts must be careful to avoid oversimplifying the claims by looking at them generally and failing to account for the specific requirements of the

claims." *McRO, Inc. v. Bandai Namco Games Am. Inc*., 837 F.3d 1299, 1313 (Fed. Cir. 2016) (internal citation omitted). Claims purporting to improve the functioning of the computer itself or improving an existing technological process are not directed to an abstract idea. *See Enfish*, 822 F.3d at 1335. Only if the claim is directed to a law of nature, natural phenomenon, or abstract idea may the court proceed to step two. *See id.* at 1334.

In the second step, a court considers whether "the elements of each claim both individually and as an ordered combination" form an "inventive concept" – that is, "an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself." *Alice Corp.*, 134 S. Ct. at 2355 (alteration in original) (internal quotations and citations omitted). An inventive concept "can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *BASCOM Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016). There is no inventive concept where the elements of the claim involve "well-understood, routine, and conventional activities previously known to the industry.'" *Alice Corp.*, 134 S. Ct. at 2359 (citation, quotation, and brackets omitted). Whether a claim element or combination is well-understood, routine, or conventional is a question of fact that must be proven by clear and convincing evidence. *See Berkheimer*, 881 F.3d at 1368.

V. ARGUMENT

A. STEP 1: THE CLAIMS ARE NOT DIRECTED TO AN ABSTRACT IDEA

1. The Claims Improve Computer-Related Technology

The authentication mechanism claimed by the '903 patent is not mere automation of a manual or mental task because it requires the activation of an authentication function that cannot be implemented without computers or computer networks. The claimed authentication method is "necessarily rooted in computer technology in order to overcome a problem specifically arising in

the realm of computer networks." *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014).

Independent claim 1 recites:

> A method of authenticating a user to a transaction at a terminal, comprising the steps of:
>
> transmitting a user identification from the terminal to a transaction partner via a first communication channel,
>
> providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,
>
> as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel,
>
> **ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,**
>
> **ensuring that said response from the second communication channel includes information that the authentication function is active,** and
>
> thereafter ensuring that the authentication function is automatically deactivated.

The '903 patent claims a solution that improves computer-related technology by increasing the efficiency of a networked authentication process, saving cost, and relieving much of the burden on the user. Rather than involving costly and time-consuming network transmissions (such as SMS messages) that require the user to retrieve, remember, and provide input for multiple authentication factors, the claims verify the user's identity by transmitting the user's identification from a terminal over a first communication channel, and using a second communication channel to check that an authentication function is activated in the user's mobile device.

As described in the '903 patent, in order to activate the authentication function, the user may for example simply turn on his mobile device so that "it connects to the nearest Base Station

Subsystem (BSS) of the mobile network . . . [and] will be identified by its device identifier (IMSI)" '903 patent at 2:54-62. No further input is needed from the user, and there is no need for the user to remember a password or input a lengthy passcode. In this case, simply turning or leaving the mobile device on is enough to determine that the authentication function is active, and querying the Home Location Register (HLR) of the mobile network is sufficient to verify the user's identity. *See id.* at 2:62-67. If the system is capable of tracking the locations of both the terminal and the mobile device, the authentication system may further check that the terminal and mobile device are at or near the same location to "provide an increased level of security," as hackers trying to impersonate a user over a computer network are unlikely to be in the same location as the user's mobile device. *See id.* at Fig. 6, 7:9-8:24.

The claimed solution increases the efficiency and reduces the cost of the computerized authentication system, and it relieves the burden on the user to remember his or her password or input the correct code. These improvements make it easier for the user to verify his or her identity, without compromising the level of security of multifactor authentication systems. Compared to conventional multifactor authentication systems, the '903 patent performs user authentication with fewer resources, less user interaction, and simpler devices. *See id.* at 1:54-56 ("[i]t is an object of the invention to provide an authentication method that is easy to handle and can be carried out with mobile devices of low complexity.") The '903 patent further states "the complexity of the authentication function can be reduced significantly . . . . [T]he only activity that is required from the user for authentication purposes is to activate the authentication function at a suitable timing for the transaction." *Id.* at 1:64-2:3. "It is a particular advantage of the invention that the mobile device does not have to have any specific hardware for capturing or outputting information. All that is required from the mobile device is that it can be activated for a certain (preferably short)

period of time and is capable of connecting to a mobile communications network." *Id.* at 2:44-9. Rather than merely automating a manual or mental process (*see FairWarning IP, LLC v. Iatric Sys.*, 839 F.3d 1089, 1095, 1296 (Fed. Cir. 2016)), or using the mobile device as a tool (*see Consumer 2.0, Inc. v. Tenant Turner, Inc.*, 343 F. Supp. 3d 581, 589 (E.D. Va. 2018)), the claims of the '903 patent improve the functionality of computers and computer networks themselves by increasing the efficiency of computerized authentication.

Claims directed to an improvement in the user's interaction with a computing device by making it more efficient are not abstract. *See Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356 (Fed. Cir. 2018). In that case, prior art user interfaces were inefficient, "requiring a user 'to scroll around and switch views many times to find the right data/functionality'" and requiring "users to drill down through many layers to get to desired data or functionality." *Id.* at 1363 (citation omitted). That process was "'slow, complex, and difficult to learn, particularly to novice users.'" *Id.* (citation omitted). The claims in *Core Wireless* provided "a specific manner of displaying a limited set of information to the user" and thereby "improve[d] the efficiency of using the electronic device" and were "directed to an improvement in the functioning of computers." *Id.* Similarly, the claims of the '903 patent improve the efficiency of an authentication system and improve the functionality of the computer itself.[1]

[1] *See also SRI Int'l, Inc. v. Cisco Sys.*, 930 F.3d 1295, 1304 (Fed. Cir. 2019) (the claims improve "the technical functioning of the computer and computer networks by reciting a specific technique for improving computer network security"); *Ancora Techs. v. HTC Am., Inc.*, 908 F.3d 1343 (Fed. Cir. 2018) (the claims are not directed to an abstract idea because "[i]mproving security – here, against a computer's unauthorized use of a program – can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem").

2. Duo Oversimplifies and Mischaracterizes the Claims

Duo fails to show that the '903 claims are directed to an abstract idea. According to Duo, "[t]he '903 Patent claims are drawn to the abstract idea of authentication." D.I. 18, at 17. This is precisely the "high level of abstraction" and "oversimplification" the Federal Circuit cautioned against in *Enfish* and *McRO*. *See Enfish*, 822 F.3d at 1337 ("describing the claims at such a high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule"); *McRO*, 837 F.3d at 1313 ("courts must be careful to avoid oversimplifying the claims by looking at them generally and failing to account for the specific requirements of the claims") (internal quotation marks and citations omitted); *see also Mod Stack LLC v. Aculab, Inc.*, C.A. No. 18-332-CFC, 2019 U.S. Dist. LEXIS 129145, at *8 (D. Del. Aug. 2, 2019) (finding that movant oversimplified the claims in *Alice* step 1). Following Duo's logic, no technology related to authentication, no matter how implemented, could ever constitute patentable subject matter. This conclusion cannot be correct.

Duo characterizes the abstract idea as multifactor authentication, arguing that humans have "verified identity using multiple factors for thousands of years," reciting a password used in the Bible, secret society handshakes and passwords, photo identification and a physical key to access a safety deposit box, and a preschool calling a parent to confirm pick-up. *See* D.I. 18, at 7-8. According to Duo, "[t]he '903 Patent implements this age-old concept [of authentication] 'in a mobile device'" *Id.* at 8. This mischaracterizes the '903 patent. The patent claims a specific way to implement authentication using mobile devices that is an improvement over the existing systems for multifactor authentication. Such claims satisfy *Alice* step 1. *See Universal Secure Registry, LLC v. Apple Inc.*, C.A. No. 17-585-CFC-SRF, 2018 U.S. Dist. LEXIS 159541 (D. Del. Sept. 19, 2018) (recommending denial of a motion to dismiss because the claims of authentication-related patents were focused on improvement of computer functionality).

The Federal Circuit has cautioned that "it is not enough, however, to merely trace the invention to some real-world analogy." *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999, 1011 (Fed. Cir. 2018). In *Data Engine*, claims directed to notebook tabs in a three-dimensional spreadsheet environment were found patent-eligible, despite the fact that "tabs existed outside the context of electronic spreadsheets prior to the claimed invention," because of "the functional improvement achieved by the specifically recited notebook tabs" and in particular because they "allow[ed] a user to avoid the burdensome task of navigating through spreadsheets in separate windows using arbitrary commands." *Id.* MDPL's claims are not merely directed to authentication, but are directed to a functional improvement achieved by the specifically-recited authentication method, which allows a user to avoid the burdensome task of having to provide multiple inputs via different channels to authenticate.

All of Duo's real-world examples demonstrate the same disadvantages of conventional authentication systems. Namely, they all require time-consuming and costly communications and burden the user to explicitly provide an input for the authentication factor. None of these examples authenticates a user by checking whether an authentication function in the user's mobile device is active. Tellingly, Duo did not, and could not, cite to any real-world example in which an equivalent of checking for an active authentication function on a mobile device was performed manually or mentally.

By contrast, the claims of the '903 patent are directed to a particular authentication mechanism where a user seeks authorization to perform a transaction at a terminal that is connected to the transaction partner via a first communication channel, and an authentication device uses a second communication channel to check an authentication function implemented on a mobile device. '903 patent at 1:3-9, 2:35-43,10:39-46. The authentication function on the mobile device

is normally inactive and activated by the user only for the transaction. *See id.* at 10:53-55. If the authentication device receives the response indicting that the authentication function on the mobile device is active within a predetermined time, the user authentication is granted. *See id.* at 10:47-60. For example, the authentication device can simply check if the user's mobile device is connected to or registered with the mobile network. *See id.* at 2:44-67.

Compared to the previously-known authentication schemes, the claimed authentication method requires less user interaction and could be implemented using simpler mobile devices. *See id.* at 1:30-56. This implementation allows the user identity to be verified without requiring that the user provide an input for each authentication factor. Instead, the system simply checks for an active authentication function on the mobile device over the second communication channel. In this manner, the claimed method removes most of the burden from the user and requires fewer computing resources as compared to conventional authentication systems.

3. Duo Contradicts Its Representations to the USPTO

Duo bases its motion on factual assertions that are outside of the pleadings – comparing the '903 patent to "age-old" authentication methods found in the Bible, secret societies, Victorian-era banks, and preschools (D.I. 18, at 7-8) – without showing how the Court may take judicial notice of them. If the Court considers Duo's factual allegations, it should also take judicial notice of the contrary representations Duo has made to the USPTO in obtaining its own authentication-related patents.[2]

[2] Because a Rule 12(c) motion for judgment on the pleadings is reviewed under the same standard as a Rule 12(b)(6) motion to dismiss (*see Revell v. Port Auth.*, 598 F.3d 128, 134 (3d Cir. 2010)), the Court may consider matters of public record that are outside of the pleadings (*see Oshiver v. Levin, Fishbein, Sedran & Berman*, 38 F.3d 1380, 1384 n.2 (3d Cir. 1994)). In a patent infringement action, a court may take judicial notice of prosecution histories, which are "public records." *Genetic Techs. Ltd. v. Bristol-Myers Squibb Co.*, 72 F. Supp. 3d 521, 526 (D. Del. 2014); *see Realtime Adaptive Streaming, LLC v. Haivision Network Video, Inc.*, C.A. No. 17-1520, 2018

Duo is listed as assignee on more than 60 issued patents and at least 2 pending patent applications related to cybersecurity, dating back as early as 2010. *See* Declaration of Leon Miniovich ("Miniovich Decl."), Ex. A. During prosecution of at least 5 of its patents and applications, Duo has argued that authentication is *not* an abstract idea and is patent-eligible. *See id.*, Ex B, at 10-14; Ex. C, at 11-12; Ex. D, at 9-10; Ex. E, at 9-11; Ex. F, at 6-7. For example, during prosecution of U.S. Patent Application No. 15/355,377 (the "'337 application"), Duo argued that the claimed digital authentication system was not directed to an abstract idea and was patent-eligible because it is rooted in computer technology, solves a problem arising out of computer technology, and cannot operate without computers:

> In any case, the Federal Circuit has clearly recognized and unambiguously stated that claimed inventions directed to technology for solving problems *necessarily rooted in computer technology* (*see DDR Holdings*) satisfy the requirements of § 101. Here, the claimed inventions are directed to methods that function to *digitally authenticate a user* and digitally approve a transaction using a push-based notification from an authentication server or computer to a digital authority device. Thus, the claimed invention *solves a problem (e.g., digital security) arising out of computer technology*. The claimed invention *cannot operate outside of the universe of computer technology* and is intended for solving problems regarding the security vulnerabilities existing in approving digital transactions and digitally authenticating a user.

Id. Ex. B, at 13 (emphasis added).

The then-pending claims of the '377 application are similar to the '903 claims, as they both attempt to improve the user's experience with the authentication platform by making it more efficient via "reduced transaction processing." *Compare id.* at 13, *with* '903 patent at 2:44-67, 3:27-33, 3:47-50. Specifically, Duo argued that the claimed push-based authentication method provides "a non-intrusive technique allowing the authentication server to interact with a registered

U.S. Dist. LEXIS 209133, at *24 (D. Del. Dec. 12, 2018) (taking judicial notice of prosecution histories of the asserted patents).

mobile device of an authorized user for obtaining additional approval and biometric authentication for the transaction." Miniovich Decl. Ex. B, at 11-12. Duo prosecuted claims directed to a multifactor authentication implemented with a mobile device – the very same concept Duo now claims is abstract. *See* D.I. 18, at 15-16. Duo cannot have it both ways. The claims of the '903 patent are not directed to an abstract concept.[3] At minimum, Duo's contrary positions show the lack of clear and convincing evidence that the patents are directed to an abstract idea, and demonstrate that there are issues of fact that preclude granting its motion.

4. Duo Relies on Cases That Do Not Improve Computer Technology and Merely Automate Manual Processes

Duo dismisses the contributions of the '903 patent as allegedly directed to the "abstract idea of authentication" and asserts "Courts have repeatedly deemed authentication claims abstract." D.I. 18, at 15. In support of what it characterizes as "settled law," Duo cites cases purportedly demonstrating that all patents related to authentication are directed to an abstract idea and are therefore are patent-ineligible. In each case, however, the ineligible claims were directed to authentication systems that merely automated a manual or mental process that could have been carried out without computers or networks, and were not directed to an improvement in computer-

[3] To the extent Duo argues that *Search & Social Media Partners* precludes consideration of its inconsistent representations to the USPTO, that case is inapplicable. MDPL offers Duo's statements from the public record to rebut Duo's statements of fact offered outside of the pleadings; Duo's statements to the USPTO confirm that the claims are not directed to abstract ideas and at minimum raise an issue of fact. Moreover, in that opinion, the court erroneously failed to acknowledge that patent prosecution histories *are* public records of which it may take judicial notice. *See Search & Soc. Media Partners, LLC v. Facebook, Inc.*, 346 F. Supp. 3d 626, 639 n.6 (D. Del. 2018); *supra* at 12 n.2. An argument that Duo's contradictory statements about its own patents do not permit a court to confer patent eligibility on otherwise ineligible subject matter, *see id.* (citing *Morsa v. Facebook, Inc.*, 77 F. Supp. 3d 1007, 1014 (C.D. Cal. 2014)), is not on point here. Duo's representations to the USPTO rebut its arguments and demonstrate the existence of fact issues that cannot be resolved at the pleadings stage.

related technology. They are unlike the facts here, where the '903 claims are rooted in and improve upon the existing computer technology.

Duo particularly focuses on the district court decisions in *StrikeForce* and *Asghari-Kamrani*. *See id.*, at 17-19. In *StrikeForce*, the claims at issue were directed to comparing transmitted data to predetermined data to determine whether to grant or deny access to a host computer. *See Strikeforce Techs., Inc. v. SecureAuth Corp.*, No. 17-cv-04314-JAK, 2017 U.S. Dist. LEXIS 222516, at *15-16 (C.D. Cal. Dec. 1, 2017). The court found that those claims "concern a long-established means of transmitting sensitive information" and the claims "are not specifically directed to an improvement in computer functionality." *Id.* at *16. Specifically, the claimed "out-of-band" authentication, *i.e.* using a separate channel to verify identity, was analogized to the "U.S. Navy tactics during World War II and ancient Greek methods for decoding and transmitting messages" and "a system for verifying identity of visitors at preschool." *Id.* at *12. Comparison of transmitted data such as an input password, to predetermined data such as a known password to determine whether to grant or deny access to a computer was "a long-established means of transmitting sensitive information," is not "distinct from any out-of-band authentication process," and is "not specifically directed to an improvement in computer functionality." *Id.* at *16. Instead, the *StrikeForce* claims "simply apply these familiar processes in the context of the use of computers that are connected to the internet." *Id.* at *17.

Duo's reliance on *StrikeForce* is unpersuasive because the '903 patent is not directed to automating a well-known "out-of-band" authentication process using computers, but rather claims a specific improvement to an existing computer network-implemented authentication scheme. The '903 patent claims are necessarily rooted in computer technology because they solve an efficiency problem that arises out of networked computers and mobile devices performing multifactor

authentication. The claims improve the functionality of the computer system itself by increasing efficiency in terms of cost and time, and relieving the burden on users.

In *Asghari-Kamrani*, the claims at issue required a user to provide a dynamic code to authenticate himself. *Asghari-Kamrani v. United Servs. Auto. Ass'n*, No. 2:15-cv-478, 2016 U.S. Dist. LEXIS 87065, at *4-5 (E.D. Va. July 5, 2016). The court found that despite the advantages presented by those claims, the problem solved by the claims was not "unique to this environment [of computer and network technology]" and its advantages "do not transform the method into one directed to an improvement of computer technology." *Id.* at *15-16. Instead, the concept of using a dynamic code to verify a transaction "could easily be performed either by hand or, more simply, with technologies much older than computers." *Id.* at *12.

In contrast, the methods claimed in the '903 patent cannot be performed by hand or with technologies much older than computers. It is not possible for a person to mentally or manually check for an activated authentication function in a mobile device over a second communication channel, which the '903 patent claims. Notably, Duo does not attempt to explain how the claims of the '903 patent could conceptually be performed by manual or mental steps, and outside of the realm of computer networks and mobile devices. Duo simply asserts that "authentication is an abstract idea" (D.I. 18, at 15), implying that *all* authentication methods are abstract.

The remaining cases Duo cites (*see id.*, at 15-16) are inapplicable for similar reasons. They are directed to automation of a mental or manual process and do not improve computer-related technology:

- Claims directed to a generic "authentication server" were abstract in view of "various pre-computer-age corollaries for which humans similarly restrict and provide access to resources." *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1016-7 (Fed. Cir. 2017).

- A method for verifying the validity of a credit card by comparing credit card numbers and internet addresses of previous transactions was abstract because all of the claimed "steps can be performed in the human mind, or by a human using a pen and paper." *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372 (Fed. Cir. 2011).

- Claims related to providing automated entry to properties via an application interface were abstract as simple "automation of a human manual process" carried out by real estate professionals for decades. *Consumer 2.0*, 343 F. Supp. 3d at 588.

- Claims directed to detecting fraud by an otherwise authorized user of patient protected health data were abstract for being similar to what "humans in analogous situations detecting fraud have asked for decades, if not centuries." *FairWarning IP, LLC v. Iatric Sys.*, 839 F.3d 1089, 1095 (Fed. Cir. 2016).

- Claims directed to tracking an object by determining whether the object is presently located within a prescribed geographic area and taking appropriate action depending on whether the object is or is not within that area were found abstract as amounting to "the same 'rule' that has always been used for determining if something is in the right place at the right time," merely automated. *CalAmp Wireless Networks Corp. v. ORBCOMM, Inc.*, 233 F. Supp. 3d 509, 513 (E.D. Va. 2017).

B. STEP 2: THE CLAIMS AMOUNT TO SIGNIFICANTLY MORE THAN AN ABSTRACT IDEA

1. The Claims Contain an Inventive Concept

The '903 claims are not directed to an abstract idea. As such, no further analysis is required, and Duo's motion should be denied. But regardless, the claims of the '903 patent amount to significantly more than an abstract idea under *Alice* step 2 because they contain an "inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application." *Alice Corp.*, 134 S. Ct. at 2357 (internal quotation marks and citations omitted).

Even if the elements recited by the '903 claims were conventional, the claimed arrangement is "non-conventional and non-generic" (*BASCOM*, 827 F.3d at 1350) and is a technological improvement over known computerized authentication systems because it accomplishes authentication using fewer resources, less user interaction, and simpler devices. *See* '903 patent at 1:54-56. Contrary to Duo's assertions (*see* D.I. 18 at 11, 24), the simplicity of the claimed mobile device requiring less user interaction is not indicative of lack of the inventive

concept, but instead provides a patent-eligible improvement over conventional authentication systems.[4] Here, the claimed authentication method improves prior art and contains an inventive concept in a non-conventional arrangement of the components, thereby reducing the amount of network transmissions needed to verify a user's identity, and increasing the efficiency of the authentication process. *See* '903 patent at 2:44-67, 3:27-33, 3:47-50. The claimed method achieves such an improvement by "provid[ing] a simpler, less expensive, and more versatile framework that is sufficiently inventive." *Elec. Scripting Prods., Inc. v. HTC Am., Inc.*, No. 17-cv-05806, 2018 U.S. Dist. LEXIS 43687, at *15 (N.D. Cal. Mar. 16, 2018).

Duo provides no rationale or support (and is unable to do so) for its conclusory argument that the combination of the claimed elements failed to provide any inventive concept. *See* D.I. 18, at 23. Rather, it takes a position that is at odds with its prior representations to the USPTO that an authentication system with efficiency improvements over existing technology *is* patent eligible. *See, e.g.*, Miniovich Decl. Ex. B, at 13 (stating that a system that achieves "the improved technical effects of reduced transaction processing and digital security in approving transactions and digitally authenticating a party to the transaction" is patent eligible). At minimum, Duo's contrary position raises an issue of fact precluding judgment on the pleadings.

2. Whether the Claimed Invention Is Well-Understood, Routine, and Conventional Is a Question of Fact

The claim limitations amount to "significantly more" when they "involve more than performance of 'well-understood, routine, [and] conventional activities previously known to the industry.'" *Content Extraction & Transmission LLC v. Wells Fargo Bank, N.A.*, 776 F.3d 1343,

[4] *See Freeny v. Fossil Grp., Inc.*, No. 2:18-cv-00049-JRG-RSP, 2019 U.S. Dist. LEXIS 36688 at *14 (E.D. Tex. Feb. 12, 2019) ("The invention improves the prior art by incorporating multiple low power type signaling capability into a single unit, and the unit delivers information in a much simpler and more convenient manner than done with existing devices and at less cost.") (internal quotation marks and citation omitted).

1347-48 (Fed. Cir. 2014) (alteration in original) (quoting *Alice Corp.*, 134 S. Ct. at 2359). As explained above, the '903 patent improves upon computer-rooted authentication technology by making it easier to verify the user's identity by increasing the efficiency without compromising the level of security. *See* Parts III, V(A)(1), V(A)(4), V(B)(1) *supra*. The question of whether that improvement was "well-understood, routine, and conventional to a skilled artisan in the relevant field is a question of fact." *See Berkheimer*, 881 F.3d at 1368; *Aatrix*, 882 F.3d at 1128. Accordingly, even if the Court determines that the '903 claims are directed to an abstract idea at step 1 and proceeds to step 2 of the inquiry, Duo's motion should be denied. *See Berkheimer*, 881 F.3d 1360; *BASCOM* 827 F.3d 1341; *Vanda Pharm., Inc. v. Roxane Labs., Inc.*, 203 F. Supp. 3d 412 (D. Del. 2016).

C. MDPL Did Not Waive Its Remaining Claims in the '903 Patent

Duo argues that MDPL does not assert claims other than claim 1 and that the Court should treat claim 1 as representative for purposes of its motion. *See* D.I. 18, at 10 & n.1. MDPL did not waive the remaining claims of the '903 patent. The amended complaint refers to claim 1 as exemplary, and it did not limit the claims against Duo exclusively to claim 1. *See* D.I. 15 ¶¶ 11, 13. A complainant need not recite every infringed patent claim in the complaint. *See Disc Disease Sol. Inc. v. VGH Sols., Inc.*, 888 F.3d 1256 (Fed. Cir. 2018). While claim 1 is one example of the asserted claims, a "claim is not representative simply because it is an independent claim." *Berkheimer*, 881 F.3d 1360 at 1365. The court should not treat claim 1 as representative of the 26 claims in the patent.

Claims 2-26 of the '903 patent pass muster under *Alice.* Each of claims 2-26 depends from claim 1 and is not directed to an abstract idea because it recites limitations that improve computerized authentication processes. Rather than reciting simply "generic computing

functionality" as Duo argues (D.I. 18, at 10), each dependent claim adds a specific technical element that increases the efficiency of the authentication system. For example:

- **Claim 4** relates to detecting an active state of the authentication function by checking only a communication register of the network, without having to communicate with the mobile device. *See* '903 patent at 2:46-67, 3:27-33. By avoiding any communications to or from the mobile device, claim 4 improves a computer-related technology by saving on costly network transmissions involving the mobile device. As such, claim 4 is not directed to an abstract idea. Claim 4 additionally involves an inventive concept because it was not well-known, routine, or conventional to check for an active authentication function on a mobile device without communicating with that mobile device.

- **Claim 5** relates to denying authentication based on the locations of the terminal and mobile device. *See* '903 patent at 2:60-67, 3:18-26, 3:50-60, 7:15-8:24. A mobile device that has been stolen is unlikely to be at the same location as the user's terminal. By checking that both the user's terminal and mobile device are at the same location, claim 5 increases the level of security of the computerized authentication process and is not directed to an abstract idea. This concept was not well-known, routine, or conventional, such that claim 5 also amounts to significantly more than an abstract idea.

- **Claim 8** relates to checking the active state of the authentication function only when the locations of the terminal and mobile device do not fulfill a spatial relationship. *See* '903 patent at 3:18-26, 7:15-8:24. By ensuring that both devices are at the same location and saving on costly network transmissions when they are at different locations, for example, claim 8 also increases the level of security and efficiency of the authentication process and is not abstract. This concept was not well-known, routine, or conventional, such that claim 8 amounts to significantly more than an abstract idea.

Duo cites *StrikeForce* to argue that the Court should treat claim 1 as representative. *See* D.I. 18, at 10. In *StrikeForce*, the plaintiff summarily stated that a claim was not representative of the other 42 asserted claims because it did not include an express "element that appears in nearly every other claim," but it did not provide "meaningful arguments" regarding that element. *See StrikeForce Techs., Inc. v. SecureAuth Corp.*, No. 17-cv-04314, D.I. 104, at 18 n.3. Here, in contrast, MDPL has advanced "meaningful arguments regarding limitations found only in the dependent claims," such that there is no waiver of those dependent claims. *Berkheimer*, 881 F.3d at 1365-66.

VI. CONCLUSION

MDPL respectfully requests that the Court issue an order denying Duo's motion.

Respectfully submitted,

POTTER ANDERSON & CORROON LLP

By: */s/ Bindu A. Palapura*

David E. Moore (#3983)
Bindu A. Palapura (#5370)
Stephanie E. O'Byrne (#4446)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19801
Tel: (302) 984-6000
dmoore@potteranderson.com
bpalapura@potteranderson.com
sobyrne@potteranderson.com

Attorneys for Plaintiff Money and Data Protection Lizenz GmbH & Co. KG

OF COUNSEL:

Scott T. Weingaertner
Stefan Mentzer
Leon Miniovich
WHITE & CASE LLP
1221 Avenue of the Americas
New York, New York 10020
Tel: (212) 819-8200

Dated: November 5, 2019
6466369 / 45431